Public Knowledge

October 21, 2016

Ms. Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554

Re: WC Docket No. 16-106

Dear Ms. Dortch:

On October 20, 2016, Harold Feld and Dallas Harris of Public Knowledge, Laura Moy of Georgetown Law's Institute for Public Representation (counsel for New America's Open Technology Institute), Natasha Duarte of Center for Democracy and Technology, Jeff Chester of Center for Digital Democracy, Kate McInnis of Consumers Union, Nathan White of Access Now, Linda Sherry of Consumer Action, Guarav Laroia of Free Press, Ariel Fox Johnson and Danny Weiss of Common Sense Kids Action, Claire Gartland of Electronic Privacy Information Center, and Jay Stanley of the American Civil Liberties Union (collectively "Privacy Advocates") met with Chairman Wheeler, Gigi Sohn, Stephanie Weiner, and Ruth Milkman of Chairman Wheeler's Office, Lisa Hone and Matthew DelNero of the Wireline Competition Bureau, and Jennifer Tatel of the Office of General Counsel with regard to the above captioned matter.

Sensitive vs. Non-sensitive

Privacy Advocates urged the FCC to stand firm on its proposal to categorize web browsing and app usage histories as sensitive. The sites visited and apps used by consumers indisputably contain information that consumers consider highly private. For example, browsing history may not only reveal information about a consumer's health status, financial status, children, or geographic location, but may also reveal information about race and gender, sexual preferences, hobbies, political views, employment status, and more.[1] App usage history can reveal similar information about consumers' private lives.[2] Advocates also noted that if the FCC's forthcoming privacy order does indeed harmonize broadband privacy rules with phone privacy rules, as the FCC has indicated it may do, then leaving browsing and app usage history off the list of sensitive information might support removal of call detail records from the sensitive category as well. This must not come to pass. Consumers would be outraged if their phone carriers were allowed to share, sell, or otherwise monetize private call records without first getting explicit opt-in consent to do so.

Privacy Advocates also urged the FCC to make clear in the final rule that the source IP address of consumers' online traffic is sensitive because it can reveal

[1] *See* OTI Notice of Ex Parte, WC Docket No. 16-106 (filed Oct. 13, 2016), at 7–8.
[2] *See id.* at 8–9.

consumers' geographic location, and that destination IP addresses are sensitive as well because they constitute browsing history. Advocates argued that MAC addresses are also sensitive information, because they are linked to consumers' devices, which—especially in the Internet of Things—can in turn reveal information about consumers' private lives. For example, MAC address data could reveal that a consumer has a connected hearing assistance device, baby monitor, or garage door opener. And traffic associated with those devices could be used to determine when, how much, and for how long consumers are using those specific connected devices.[3]

In addition, in the event the FCC includes an enumerated list of types of information deemed "sensitive" under its broadband privacy rules, advocates encouraged the FCC to make clear that the enumerated list is neither final nor exhaustive. We cannot anticipate every privacy concern that will arise as technology advances, but we can be confident that there will be new concerns, including around new categories of data or new uses of existing categories of data.

De-Identified Information

Privacy Advocates expressed concern that the exception for de-identified data could become an exception that swallows the rule. Current targeted advertising practices often relies on nominally de-identified data, so heightened protections for browsing history and app usage could be undermined by this exception. Advocates urged the Commission to require some form of consumer consent for the use of de-identified data, preferably opt-in consent but at minimum opt-out consent. Advocates explained that requiring consent would encourage transparency of de-identification techniques. If the Commission does proceed with this exception, Advocates urged the Commission to maintain oversight and enforcement authority and to ensure independent verification of de-identification techniques. The FCC should ensure that legal standards for de-identification best practices evolve as techniques for de-identification and re-identification evolve. Advocates also explained that the definition of de-identified data should be expanded to require that information cannot be linked or linkable to any unique identifier or pseudonym. Further, the FCC should clarify its authority to how ISPs liable if third parties who receive de-identified data fail to uphold commitments not to re-identify that data, potentially via 47 U.S.C. § 217.

Mandatory Arbitration

In the wake of the Ninth Circuit's recent decision in *AT&T Mobility v. FTC*, the Commission has lost a valuable partner in protecting the privacy of broadband subscribers. Furthermore, the Commission relies exclusively on private rights of action and class actions to enforce MVPD privacy under 47 U.S.C. §§ 338(i) & 551. Without the ability to sue for relief in court, consumers have no replacement for the loss of the FTC as a partner with the FCC. Furthermore, the proliferation of mandatory arbitration

[3] *See id.* at 4–6.

clauses effectively forecloses consumers from enforcing their rights under 47 U.S.C. §§ 338(i) & 551.

There is evidence in the record documenting the ubiquity of mandatory arbitration clauses in telecommunications service contracts and the harm they cause to consumers.[4] In addition to the evidence in the record, the Consumer Financial Protection Bureau conducted a three- year examination on the use of forced arbitration in the consumer financial services sector.[5] The study data and agency findings are a strong indicator of how forced arbitration impacts customers in telecommunications, including for broadband privacy claims.

Prohibiting mandatory arbitration clauses is particularly warranted in this context for several reasons. Section 222 and 47 U.S.C. §§ 338(i) & 551 are inextricably linked. The cable privacy provisions apply to any service that is delivered over the same infrastructure, which includes broadband. The Commission has long relied on private rights of action to enforce the 47 U.S.C. §§ 338(i) & 551. Because of the connection between the privacy provisions, allowing mandatory arbitration clauses in privacy policies would have an impact on consumer's privacy rights beyond 47 U.S.C. § 222. Further, ISPs maintain consumer information and assume the risk by demanding that consumers opt-out instead of opt-in. If ISPs insist on collecting large amounts of consumer data on an opt-out basis, they must be accountable to consumers when their privacy is violated.

The Commission should therefore use its authority pursuant to Section 201(b), 338(i) and 631 to prohibit enforcement of mandatory arbitration clauses. At a minimum, even if the Commission were to determine that it did not intend to prohibit such clauses based on the record, the Commission should clarify that it has such authority and will revisit its determination if evidence of the abusive effects of these clauses becomes more manifest.

Pay for Privacy

Many of Privacy Advocates have called for "pay for privacy" to be banned as an unjust and a unreasonable practice. Privacy Advocates noted that the fact sheet indicates the FCC will likely take a different approach, instead merely requiring heightened disclosure for costumers and examining the reasonableness and sufficiency under the rules of various pay for privacy offers on a case-by-case basis. Privacy Advocates urged

---

[4] *See e.g.*, NACA et al. Ex Parte; Comments of National Association of Consumer Advocates, et al.; Ex Parte New America's Open Technology Institute, ACLU, Free Press, Center for Democracy & Technology, Center for Digital Democracy, Common Sense, Electronic Privacy Information Center, Consumer Federation of America, Consumer Watchdog (September 12, 2016).

[5] Consumer Financial Protection Bureau, *Arbitration Study: Report to Congress* 2015, *available at* http://www.consumerfinance.gov/data-research/research-reports/arbitration-study-report-to-congress-2015/.

the Commission to ensure that ISPs are not permitted to charge their customers premiums for privacy that customers are not reasonably able to take advantage of. Such premiums would undermine customers' statutory entitlement to consent or refuse to provide consent for non-service-related uses of their data. Pay-for-privacy premiums could also constitute a *de facto* "take-it-or-leave-it" offering for customers, in which privacy protections are so unaffordable as to be effectively unavailable to some customers, who then are forced either to grant permission for undesirable privacy invasions, or to forego service. Privacy Advocates commended the FCC for including a provision that prohibits "take it or leave it" for ISPs privacy policies.

EU Privacy Shield

In 2015, in the wake of the Snowden revelations, the EU Court of Justice struck down the existing agreement between the United States and the EU that permitted companies to transfer personal information out of Europe to the United States consistent with the EU Privacy Directive.[6] The United States Department of Commerce and the European Union negotiated a new "Privacy Shield" agreement that relies upon regulations, self-certification and enforcement in the United States to provide adequate standards of protection for personally identifying information (PII) of European citizens.[7] Whether the EU Court of Justice will consider the Privacy Shield adequate remains to be seen.

An additional complication has emerged within the last week as the EU Court of Justice has determined that dynamic and static IP addresses are PII subject to the EU Privacy Directive and therefore, of course, subject to the restrictions of Privacy Shield. The proposed treatment of browser history and application history as "non-sensitive," appears likely to significantly undermine the adequacy of the Privacy Shield for the EU Court of Justice. By contrast, treatment of browser history and application history as sensitive information will likely enhance the acceptability of the Privacy Shield.

To understand why, it is important to keep in mind two things. First, "browser history" and "application history" are a stored collection of IP addresses and associated metadata. They are valuable precisely because the IP address identifies the source or destination of the transmission.[8] Second, by tracking browser history and application history without express consent, by storing and examining application history and

---

[6] https://www.wired.com/2015/10/tech-companies-can-blame-snowden-data-privacy-decision/

[7] https://www.commerce.gov/page/eu-us-privacy-shield, http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_eu-us_privacy_shield_en.pdf.

[8] PK does not assert that an IP address or other identifier is proof positive of identification in all circumstances. Indeed, the ability to forge an IP address is well established. But the ISP is in a unique position to use the IP address as an identifier because it is the ISP that assigns the IP address (in the case of a dynamic IP address) and that completes the routing to the end user.

browser history for traffic inbound from the EU or outbound to the EU, ISPs store and use EU PII without regard to the Privacy Shield. Worse for US companies that do certify under Privacy Shield, their information must invariable pass through ISPs (third parties) who have access to the IP addresses inbound from or outbound to the EU.

PK does not state definitively that classifying IP addresses – whether as part of browser history or application history – automatically violates the requirements of the Privacy Shield. Rather, PK urges that the Commission implement the regulatory regime that is most conducive to compliance with the EU Privacy Directive and Privacy Shield. Under Section 303(r), the Commission has both the authority and the responsibility to implement the provisions of any international agreement relating to communication by wire and wireless.[9] At a minimum, the Commission should avoid adopting a regulatory framework for ISP privacy which would raise a cloud over the Privacy Shield when it has only just been agreed to and implemented.

In accordance with Section 1.1206(b) of the Commission's rules, this letter is being filed with your office. If you have any further questions, please contact me at (202) 861-0020.

Respectfully submitted,

/s/ Dallas Harris
Dallas Harris
Policy Fellow
Public Knowledge
1818 N Street, NW
Washington, DC 20036

[9] 47 U.S.C. §303(r). Accordingly, even though the Commerce Department is charged under the agreement with ensuring compliance with the certification regime, the FCC has both a statutory authority and responsibility to ensure that the United States properly implements Privacy Shield with regard to the actual transfer of data.